ORIGINAL

FILED
NOV 15 3 34 PM '95
RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA. S.J.

119

MICHAEL M. CARLSON (Bar No. 88048)
BRYAN J. WILSON (Bar No. 138842)
JANA G. GOLD (Bar No. 154246)
Morrison & Foerster
755 Page Mill Road
Palo Alto, California 94304-1018
Telephone: (415) 813-5600
Facsimile: (415) 494-0792

PATRICK J. FLINN (Bar No. 104423)
ALSTON & BIRD
One Atlantic Center
1201 West Peachtree Street
Atlanta, Georgia 30309
Telephone: (404) 881-7000
Facsimile: (404) 881-8777

Attorneys for Proposed Intervenor
CARO-KANN CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROGER SCHLAFLY,

Plaintiff,

v.

PUBLIC KEY PARTNERS and RSA DATA SECURITY, INC.,

Defendants.

No. CV 94 20512 SW

CKC'S OPPOSITION TO SCHLAFLY'S MOTION FOR SUMMARY JUDGMENT; AND CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

Date: December 6, 1995
Time: 10:00 a.m.
Hon. Spencer Williams

TABLE OF CONTENTS

TABLE OF AUTHORITIES

RULES

STATUTES

MISCELLANEOUS

NOTICE OF CROSS MOTION FOR SUMMARY JUDGMENT

PLEASE TAKE NOTICE that on December 6, 1995, (Proposed) intervenor/defendant Caro-Kann Corporation ("CKC") will, and hereby does, cross-move for summary judgment that United States Patents Nos. 4,200,770 ("Diffie-Hellman") and 4,218,582 ("Hellman-Merkle") are not invalid in view of (1) allegations that the Diffie-Hellman patent is subject to a statutory bar; (2) allegations that the Diffie-Hellman and Hellman-Merkle patents are invalid because they claim non-statutory subject matter; (3) allegations that the Hellman-Merkle patent is inoperative because the "trapdoor knapsack" problem described in the specification has been broken.

MEMORANDUM OF POINTS AND AUTHORITIES

Introduction. Until its dissolution on September 6, 1995, defendant Public Key Partners ("PKP") held exclusive sublicensing rights to the four patents that are the subject of Mr. Schlafly's motion for summary judgment. After PKP was dissolved, control of two of the patents, United States Patent Nos. 4,200,770 ("Diffie-Hellman") and 4,218,582 ("Hellman-Merkle") went to CKC. Control of the other two patents, United States Patent Nos. 4,405,829 ("RSA") and 4,995,082 ("Schnorr") went to Caro-Kann's partner, RSADSI. RSADSI is addressing Schlafly's claims with respect to the RSA and Schnorr patents. This Memorandum addresses Schlafly's arguments with respect to the Diffie-Hellman and Hellman-Merkle patents.[1]

---

[1] CKC understands that Plaintiff's motion addresses only the validity of the Schnorr patent, and not the scope of the Schnorr claims, or whether those claims cover practice of DSS. CKC takes no (Continued)

Those arguments, and the undisputed facts of this case, establish that none of Schlafly's allegations are sufficient, as a matter of law, to support a claim that the Diffie-Hellman and Hellman-Merkle patents are invalid. Accordingly, CKC opposes and cross-moves for summary judgment on those claims.

STATEMENT OF FACTS

Public Key Cryptography. The patents at issue in this case represent one of the most fundamental advances in the field of cryptography since the invention of the alphabet substitution cipher (Omura Decl. ¶ 2). Before 1976, all cryptographic code schemes used a single "key" both to encode and decode a message (Id.). Two parties who wished to communicate over an open, or insecure, channel needed to find a way to exchange the cryptographic key before a coded message could be sent (Id.). Besides being cumbersome, the security of the message depended on the security of the means by which the key was exchanged (Id.).

In 1976, Stanford University Professor Martin Hellman, with the assistance of his graduate student Whitfield Diffie devised systems by which two parties, who could only communicate over an insecure channel, could nonetheless compute a shared secret number without the need to have a secret key delivered to both ends (Omura Decl. ¶ 2). Later, with the additional help of then-student Ralph Merkle,

---

(Continued from previous page)
position regarding Schlafly's claims regarding the validity of the Schnorr patent. CKC notes, however, that PKP no longer has any rights in the Schnorr patent (Gold Decl. Exh. G), and thus there does not appear to be a justiciable controversy between plaintiff and PKP on that subject. PKP has no infringement counterclaim pending against plaintiff on the Schnorr patent.

Professor Hellman developed a method of encryption in which (1) messages could be encoded with one key, and decoded with a second key, and (2) knowledge of one key would not allow a third party to learn or obtain the other key (Id.).

Under the system Hellman and his students envisioned, each user would have two keys: a "public" key associated with the individual and known to all, and a "secret" or "private" key known only to the individual (Omura Decl. ¶ 3). The public and private key would be related in such a way that it would be easy to generate a public key from the private key, but "computationally infeasible" to derive the private key from the public key (Id.). Thus, a sender could encrypt a message using the recipient's public key; once the message was encrypted, however, the only way to decrypt the message would be to use the recipient's private key (Id.).

The application of the Stanford patents goes far beyond their use in encrypting messages (Omura Decl. ¶ 4). For example, the techniques associated with the Diffie-Hellman patent make it possible to manage keys for users on an encrypted network without requiring delivery of the secret keys (Id.). More importantly, the techniques associated with the Hellman-Merkle patent make it possible to verify whether a particular message was actually sent by a particular party by using "digital signatures" (Id.). If the party sending the message "signs" it by encrypting a signature using her private key, then that person's public key will decrypt it (Id.). Put another way, if the sender's public key decrypts the signature, then the recipient can be certain that the message was encrypted by that sender's private key (Id.).

Public Key systems—and particularly digital signatures—have come to have important applications with the advent of electronic commerce (Omura Decl. ¶ 5). Commercial transactions over electronic networks can be signed and verified, obviating the need for paper verification (Id.).

The Diffie-Hellman Patent.[2] The first of the two patents at issue in this memorandum covers what has been called the "Diffie-Hellman" key exchange (Omura Decl. ¶ 6, Exh. A; Gold Decl. Exh. H). The Diffie-Hellman key exchange method was conceived before any complete embodiment of Public Key, and is often called a precursor to Public Key cryptography (Id.). Diffie-Hellman teaches a way of exchanging numbers over an insecure channel and calculating a shared, secret number from the nonsecret numbers (Id.). This technology is often used in computer communication networks, for example, to electronically obtain keys to secure communications of users who wish to connect to the network (Id.).

In its broadest terms, the Diffie Hellman patent claims a system where each party starts out with a secret number (Omura Decl. ¶ 7). Using a one-way function (that is, a function which is easy to perform but difficult to invert), each party generates a nonsecret number from their secret number (Id.). The parties then exchange their nonsecret numbers (Id.). Once the nonsecret numbers are exchanged, each party calculates the key from their retained,

---

[2] Although the patent is popularly referred to as "Diffie-Hellman" and we adopt that term here, the invention was made by (and the patent issued to) Hellman, Diffie, and Merkle (Gold Decl. Exh. H).

secret number, and the other party's exchanged nonsecret number (Id.). As disclosed in the Diffie-Hellman patent, the exchanged secret/nonsecret numbers will enable the parties to calculate a common key without having to exchange the key over an insecure communications channel (Id.).

The Hellman-Merkle Patent. Hellman-Merkle is the fundamental, patent covering the practice of Public Key cryptography (Omura Decl. ¶ 8, Exh. B; Gold Decl. Exh. I). Hellman-Merkle includes broad claims (claims 1-6) that cover the use of Public Key regardless of the type of encryption algorithm used to generate the public-private key pairs (Id.). Thus, the Hellman-Merkle patent discloses and claims the use of two different keys, one for encoding the information, and the second for decoding the information (Id.). Under this system, one who wishes to receive a coded message may publish a "public key" to the world at large (Id.). Anyone wishing to send this person a coded message uses the individual's public key to encode the message (Id.). The recipient, using the corresponding, but secret, "private key" decodes the message (Id.). Because the public key only works to encode the message, and only the secret private key can decode the message, the disclosure of the public key does not affect the secrecy of the message; only the holder of the private key (the recipient) can open the message.

The particular implementation of Public Key described in the patent specification uses a mathematical function known as the "knapsack problem" (Omura Decl. ¶ 9). Claims 7-17 cover various implementations of Public Key involving various forms of the knapsack problem (Id.).

The "Multiuser Cryptographic Techniques" and "New Directions" Papers. Professor Hellman and Whitfield Diffie published two papers generally disclosing the concept of Public Key cryptography in 1976. The first was called "Multiuser Cryptographic Techniques" and was published in June 1976 as part of the proceedings of the National Computer Conference (AFIPS Conference Proceedings, Vol. 45 (Omura Decl. Exh. C)). The second was the paper "New Directions in Cryptography," published in the journal IEEE Transactions on Information Theory, Vol. 22, No. 6 in November, 1976 (Id. Exh. D). Both of these papers were disclosed to and considered by the Patent Office, and the patents were granted over them (Gold Decl. Exhs. H and I).

The "Multiuser Cryptographic Techniques" paper suggested the concept of Public Key cryptography by proposing that the problem of key distribution could be solved by giving each user a pair of keys, one public and one private (Omura Decl. ¶ 11, Exh. C at 110). The paper did not, however, disclose any particular implementation that would enable one skilled in the art to make such a system work (Id. ¶ 11). Indeed, the paper noted that "[a]t present, we have neither a proof that public key systems exist, nor a demonstration system" (Id., Exh. C at 111).

The "New Directions" paper, published by the IEEE in November 1976 went only a little bit further toward disclosing the fundamental Public Key invention (Omura Decl. ¶ 12). In the "New Directions" paper, Diffie and Hellman described two possible solutions to the problem of ensuring secure communications over insecure channels (Id. Exh. D at 647). The first possible solution

was the Public Key invention—that is, a system where each user would have a public and a private key (Id. at 648). Again, however, Diffie and Hellman admitted that their only example of a possible public key cryptosystem was "[a] suggestive, although unfortunately useless example" (Id.). The second technique suggested in the "New Directions" paper was the public key distribution system set forth in the Diffie-Hellman patent (Id. at 648-49). This part of the "New Directions" paper did include a complete description of a system that would enable one skilled in the art to put together a key distribution system like the one later claimed in the Diffie-Hellman patent (Id.).

Both the Diffie-Hellman and Hellman-Merkle patent applications were filed well within a year of the November 1976 publication of the "New Directions" paper (Gold Decl. Exhs. H and I).

ARGUMENT

I. SCHLAFLY'S BURDEN ON SUMMARY JUDGMENT REQUIRES CLEAR AND CONVINCING, ADMISSIBLE EVIDENCE

The Diffie-Hellman and Hellman-Merkle patents are presumed valid. 35 U.S.C. § 282. In order to overcome that burden on his motion for summary judgment—or in opposition to this cross-motion, Schlafly will have to present clear and convincing evidence of invalidity. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986) (substantive burden carries over to motion for summary judgment); Avia Group Int'l Inc. v. L.A. Gear California, 853 F.2d 1557 (Fed. Cir. 1988)(patentee entitled to summary judgment on issue of validity). The presumption of validity is particularly difficult to overcome where, as here, the Patent Office has considered and

rejected many of the arguments advanced by the party challenging the patents. Hewlett-Packard Co. v. Bausch & Lomb, Inc., 909 F.2d 1464, 1467 (Fed. Cir. 1990) (burden of showing the invalidity of patent claims is "especially difficult when the prior art was before the PTO examiner during prosecution of the application").

The evidence in support of (or in opposition to) the motion for summary judgment must also be admissible.[3] Beyene v. Coleman Sec. Services, Inc., 854 F.2d 1179, 1181 (9th Cir. 1988). Unauthenticated documents are not admissible in a motion for summary judgment any more than they would be at trial. Id., Fed. R. Evid. 901. Similarly, hearsay statements or opinions cannot be used to support Schlafly's burden on summary judgment. Horta v. Sullivan, 4 F.3d 2, 8 (1st Cir. 1993) (newspaper articles were hearsay and not be used in evidence on motion for summary judgment). There is no admissible evidence offered in support of Schlafly's arguments, and those arguments must be rejected as a matter of law.[4]

---

[3] CKC and PKP have filed Objections to Evidence proffered by Schlafly in a separate document.

[4] The fact that Schlafly is a pro se litigant does not permit him to ignore the rules of evidence or procedure. Jacobson v. Filler, 790 F.2d 1362, 1364-65 (9th Cir. 1986).

II. THE DIFFIE-HELLMAN PATENT IS NOT SUBJECT TO A STATUTORY BAR.

Schlafly argues that the Diffie-Hellman patent is invalid under 35 U.S.C. § 102(b) because there was a public disclosure of the invention more than one year prior to the patent application (Schlafly Motion at ¶ 3.1). Section 102(b) denies patentability if "the invention was . . . described in a printed publication in this or a foreign country . . . more than one year prior to the date of the application for patent in the United States." It is undisputed that the Diffie-Hellman patent application was made on September 6, 1977 (Id., Gold Decl. Exh. H). There is no admissible evidence in this case, however, that the Diffie-Hellman invention was described in a printed publication more than one year prior to that date.

The question of whether a document constitutes a "printed publication" is one of law. Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1568 (Fed. Cir. 1987). The test for whether a disclosure has been "published" turns on the public accessibility of the disclosure, that is, whether:

> it has been disseminated or otherwise made available to the extent that persons interested and of ordinary skill in the subject matter or art, exercising reasonable diligence can locate it and recognize and comprehend therefrom the essentials of the claimed invention.

Massachusetts Institute of Technology v. AB Fortia, 774 F.2d 1104, 1109 (Fed. Cir. 1985). In addition, to render the patent invalid under § 102(b), the printed publication must be "enabling"—that is, the publication must be sufficient to allow one of ordinary skill in

the art to reproduce the claimed invention. 1 Chisum Patents § 3.04[1].

Schlafly makes several allegations in support of his argument that the invention was disclosed in a printed publication more than one year before the allegation. The first is that the invention was disclosed when the "New Directions" paper was submitted to the IEEE in June, 1976 (Schlafly Motion at ¶ 3.2). As this Court has held, however, submission of a paper to the IEEE does not constitute publication. National Semiconductor Corp. v. Linear Technology Corp., 703 F.Supp. 845, 847-49 (N.D. Cal. 1988) (IEEE policy does not permit submitted papers to be treated as "publicly available").

Second, Schlafly alleges that co-inventor Whitfield Diffie published a paper in 1988 in which he stated that the "New Directions" paper had been distributed and discussed in June 1976 (Schlafly Motion ¶ 3.3). The statement Schlafly presumably refers to actually reports only the following:

> Marty and I immediately recognized that we had a far more compact solution to the key distribution problem [in the Diffie-Hellman key exchange] than Merkle's puzzles and hastened to add it to both the upcoming National Computer Conference presentation and to "New Directions." The latter not contained a solution to each aspect of the public key problem, though not the combined solution I had envisioned. It was sent off to the IEEE TRANSACTIONS ON INFORMATION THEORY prior to my [June 1976] departure for NCC and like all of our other papers was immediately circulated in preprint.

Gold Decl. Exh. J ["The First Ten Years of Public-Key Cryptography," Proceedings of the IEEE, Vol. 76, No. 5, May 1988, p. 563].

This statement is, of course, hearsay, and is not admissible to show that copies of the paper were, in fact, "published" prior to September, 1976. Moreover, the author of the statement, when deposed in the Schlafly litigation, illustrated the risk of relying on hearsay, when he testified that the "First Ten Years" article was simply wrong on this point:

> Q BY MR. SCHLAFLY: Okay. I'm particularly interested in the last sentence, where it says: "like all of our papers was immediately circulated in preprint." What did this mean?
>
> [Objection]
>
> Q BY MR. SCHLAFLY: Okay. Is that a correct statement?
>
> A I believed it was at the time I wrote it, no longer believe so and found I couldn't defend it.
>
> Q Do you think that's a false statement?
>
> A I believe it is a false statement.

Gold Decl. Exh. K (Diffie Dep. at 84:18-85:3).

Schlafly's third allegation, similarly, is both unsupported by admissible evidence and contradicted by the direct testimony of the inventors. The purported "preprint" offered by Schlafly as Exhibit CA is entirely unauthenticated and cannot be admitted in support of this motion. Fed. R. Evid. 901(a); Canada v. Blain's Helicopters Inc., 831 F.2d 920, 925 (9th Cir. 1987) ("documents which have not had a proper foundation laid to authenticate them cannot support a

motion for summary judgment").[5] More importantly, its status as a "preprint" has been expressly contradicted by Mr. Diffie, who testified that he believed that the August date on the cover indicated that the document was a revision made at the request of the reviewing committee to conform the citation format of the submitted paper (Gold Decl. Exh. K [Diffie Dep. at 41:12-13, 42:24-43:21). Dr. Hellman, meanwhile, could not authenticate the document at all, much less verify that he had distributed it to anyone (Id., Exh. L [Hellman Dep. at 164:5-165:2]).

Mr. Schlafly's fourth allegation is that Professor Hellman lectured on the invention at a 1976 symposium in Sweden (Schlafly Motion at ¶ 3.5). Schlafly offers no evidence as to the contents of the presentation, and no evidence that any paper was "published" at the conference.[6] Indeed, Dr. Hellman has testified that he does not believe that he distributed any printed material at the conference or that he even had the "New Directions" paper with him at the conference(Gold Decl. Exh. L [Hellman Dep. 35:17-25; 36:25-37:3]).

---

[5] Schlafly alleges that he obtained this document from an IBM engineer. Even accepting this representation as true, there is no evidence regarding when or how the engineer obtained the paper; to the extent that Mr. Schlafly implies that the engineer obtained the article prior to September 6, 1977, the evidence is pure inadmissible hearsay.

[6] At Dr. Hellman's deposition, Mr. Schlafly represented that Exhibit GH to his motion was an abstract from the conference (Gold Decl. Exh. L [Hellman Dep. at 22:19-23:25, 34:22-35:1]). Exhibit GH, however, appears to be missing over 30 pages, and could not be authenticated as an abstract connected with the Sweden conference by Dr. Hellman (Id. [Hellman Dep. at 23:21-25, 34:22-35:1]). Accordingly, the exhibit is inadmissible to the extent that it is being offered as an abstract of the presentation made at the Sweden conference. Fed. R. Evid. 901.

Although there may have been a published abstract distributed by the organizers of the conference (Id. [Hellman Dep. 34:22-35:16]), there is no evidence that any such abstract would have been sufficient to enable one skilled in the art to reproduce the invention claimed in the Diffie-Hellman patent. See Ecolochem, Inc. v. Southern California Edison Co., 863 F. Supp. 1165, 1177 (C.D. Cal. 1994), citing In re Hall, 781 F.2d 897, 899 (Fed. Cir. 1986).

In sum, Schlafly has not adduced any admissible evidence that the Diffie-Hellman invention was disclosed in a printed publication more that one year before the application date of September 6, 1977.[7] Rather, the only admissible evidence of record shows that authors of the paper limited access to copies of the "New Directions" paper (Gold Decl. Exhs. L [Hellman Dep. 37:8-17; 38:23-] and K [Diffie Dep. 43:5-13, 45:25-46:3; 84:18-85:3; 86:19-22]). No member of the public had direct access to a copy of the manuscript and there is no evidence that the paper was catalogued or distributed prior to actual publication in a way that would allow persons of ordinary skill to access the paper.

Given these restrictions, the alleged pre-publication disclosures cannot constitute "publication" within the meaning of the statute. Compare Northern Telecom, Inc. v. Datapoint Corp., 908

---

[7] Schlafly further alleges that the PTO was not informed of these prior art disclosures (Schlafly Motion at ¶ 3.6). It is not clear what "disclosures" Mr. Schlafly is referring to. However, to the extent he refers to the National Computer Conference and Sweden conference alleged in ¶¶ 3.4-3.5, the statement is false. The fact that the paper had been discussed at these two conferences is disclosed in the "New Directions" paper, which was before the Patent Office during the prosecution of the patent (Gold Decl. Exh. H at 102).

F.2d 931, 936 (Fed. Cir. 1990) (distribution of 50 copies of document did not constitute publication when the document was distributed under an understanding that copies would not be disseminated and where members of public did not have direct access to the document) and In re Cronyn, 890 F.2d 1158, 1159(Fed. Cir. 1989) (undergraduate thesis in college library was not "publication" even though thesis and index was available to public) with Massachusetts Institute of Technology v. AB Fortia, 774 F.2d 1104, 1109 (Fed. Cir. 1985) (dissemination of copies of conference paper at conference "without restriction" held to be publication). Nor has Schlafly adduced or presented any evidence that any of the alleged "publications" would have enabled the invention claimed in the Diffie-Hellman patent. Accordingly, the Diffie-Hellman patent is not invalid under the publication bar of 35 U.S.C. § 102(b).

III. NEITHER DIFFIE-HELLMAN, NOR HELLMAN-MERKLE, ARE INVALID AS NON-STATUTORY SUBJECT MATTER

Schlafly alleges that the Diffie-Hellman and Hellman-Merkle patents are invalid because they claim non-statutory subject matter (Schlafly Motion ¶¶ 3.7 and 4.10). According to Schlafly, both patents can be "readily seen" to consist purely of "mathematical formulas" (Id.). The question of whether the patents claim nonstatutory subject matter can be resolved as a matter of law

In point of fact, none of the claims of either patent consists of a purely mathematical formula (Omura Decl. ¶ 13). Indeed, in the Diffie-Hellman patent, the only claim that includes a mathematical formula is claim 8, which claims "an apparatus for generating a secure cipher key, comprising ..." (Id.). In the Hellman-Merkle

patent, similarly, the first six claims do not include any mathematical formula at all, and claims 7-17 all claim either an "apparatus" or "a method" (Id.). Nor does the inclusion of a mathematical formula in the claims render them invalid. As the Supreme Court has observed, "a claim drawn to subject matter otherwise statutory does not become nonstatutory merely because it uses a mathematical formula." Diamond v. Diehr, 450 U.S. 175, 187 (1981).

Rather, "the proper inquiry in dealing with the so called mathematical subject matter exception to § 101 . . . is to see whether the claimed subject matter as a whole is a disembodied mathematical concept . . .." In re Alappat, 33 F.3d 1526, 1544 (Fed. Cir. 1994) (emphasis in original) (in bank); see also In re Iwahashi, 888 F.2d 1370, 1374-75 (Fed. Cir. 1989) ("Freeman-Walter" test developed by Court of Appeals looks at whether claim as a whole preempts an algorithm or whether algorithm is merely implemented in a specific manner). Thus

> When a claim containing a mathematical formula implements or applies that formula in a structure or process which, when considered as a whole, is performing a function which the patent laws were defined to protect, (e.g. transforming or reducing an article to a different state or thing), then the claim satisfies the requirements of §101.

Diamond v. Diehr, 450 U.S. at 192 (emphasis added).

In this case, there cannot be any dispute that the claims of both patents are directed to methods (and apparatus) for transforming messages from one state to another, and from one party

to another (Omura Decl. ¶ 13). The fact that these messages are comprised of information bits rather than some more transparently physical phenomenon does not, contrary to Mr. Schlafly's contention, render them any less patentable. See Alappat, 33 F.3d at 1544 ("fact that the four claimed means elements function to transform one set of data to another through what may be viewed as a series of mathematical calculations" does not justify rejection of claims); Iwahashi, 888 F.2d at 1375 (claim of apparatus for processing signals for patter-recognition directed to statutory subject matter).[8]

The Diffie-Hellman patent does not preempt Mr. Schlafly or anyone else from using the discrete logarithm problem incorporated in claim 8, except when they use it in "an apparatus for generating a secure cipher key" and where the algorithm is used as a means for generating the "third" and "fourth" signals described by the patent (Omura Decl. ¶ 14). Diamond v. Diehr, 450 U.S. at 187. Similarly, Hellman-Merkle does not preempt the use of knapsack algorithms unless it is being used to generate a public key from a private number in a system or apparatus for communicating securely over insecure channels (Id.). Rather, the patents seek "only to foreclose from others the use of that equation in conjunction with

---

[8] Schlafly contends that any hardware associated with the patents is "not novel" and thus, presumably cannot rescue the claims. Apart from being factually wrong, this contention is irrelevant as a matter of law. In Diamond v. Diehr, the Court held unequivocally that "the 'novelty' of any element or steps in a process, or even the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter." 450 U.S. at 188-189.

all of the other steps in their claimed process." 450 U.S. at 187. Accordingly, CKC is entitled to judgment as a matter of law that the claims of the Diffie-Hellman and Hellman-Merkle patents are not invalid for failure to claim statutory subject matter under 35 U.S.C. § 101.

IV. HELLMAN-MERKLE IS NOT INOPERATIVE UNDER ANY LEGAL DEFINITION OF OPERABILITY.

Schlafly contends that the Hellman-Merkle knapsack system was "broken" by attacks made on the system after its first publication in 1978 and that the patent is, therefore, invalid. It is undisputed that in 1982, Dr. Merkle paid $100 to a researcher who attacked a class of knapsacks, called "single iteration" knapsacks, and in 1984, Dr. Merkle paid $1000 to another researcher who attacked so-called "low density multiple iteration knapsacks" (Schlafly Motion ¶¶ 4.2-4.4). According to Schlafly, these facts prove that the knapsack problem has been "broken" and means that the Hellman-Merkle patent is invalid because it is inoperative as disclosed.[9] Schlafly is wrong on both counts and PKP and CKC are entitled to judgment on this claim.

---

[9] Although there is no dispute that Professor Merkle paid $100 and $1000 bets, the only evidence Schlafly produces on this point is a series of newspaper and journal articles (Exhs. CB, CC, CD, and CK. Each of these documents is hearsay and cannot be admitted for the truth of the matters asserted therein. See, e.g. Horta v. Sullivan, 4 F.3d at 8-9 (newspaper article inadmissible as evidence supporting summary judgment motion); Joiner v. General Elec. Co., 864 F.Supp. 1310, 1317 (N.D. Ga. 1994) (learned treatises are inadmissible hearsay on motion for summary judgment unless they are relied upon by expert).

Preliminarily, as a matter of fact, there is no evidence that the knapsack problem as disclosed and claimed in the patent has been "broken." The Hellman-Merkle specification teaches the use of multiple iteration knapsacks as the best mode of practicing the invention (Gold Decl. Exh. M [Merkle Dep. 98:2-100:19; 102:6-15); Omura Decl. Exh. B at Col. 16, lines 46-53). Even the winner of the $1000 prize did not claim to have broken all types of multiple iteration knapsacks; rather, he only claimed to have attacked some kinds of "low density" multiple iteration knapsacks (Gold Decl. Exh. M [Merkle Dep. 135:5-23]; Exh. N [Merkle Dep. Exh. M-13). Moreover, those multiple iteration knapsacks which the author did claim to have attacked required as much as 347,000 hours (about 40 years) of Cray computer time (Id.). In short, even the use of low density multiple iteration knapsacks would protect the user from attack by all but those few individuals possessed of extraordinary encryption resources. See Engle Indus., Inc. v. Lockformer Co., 946 F.2d 1528 (Fed. Cir. 1991) ("The enablement requirement is met if the description enables any mode of making and using the claimed invention").[10]

More importantly, Schlafly's attack on the Hellman-Merkle patent fails as a matter of law for at least three reasons, even if one assumes that the knapsack problem has been "broken." First, the

---

[10] Dr. Merkle testified that he did not believe that the claimant of the $1000 prize had, in fact, broken the multiple interated knapsack program. He paid the prize, however, because it would have taken him a substantial effort to disprove the attack, because he could not justify that effort, and because, under such circumstances, he considered that it would be "unsportsmanlike" to withhold the award (Gold Decl. Exh. M [Merkle Dep. 131:11-132:24]).

first six claims of the Hellman-Merkle patent read broadly on the practice of Public Key technology, regardless of the algorithm used to generate the public private key pair (Omura Decl. ¶ 8). The specification makes it clear that the use of the knapsack problem is "an example system" (Omura Decl. Exh. B, Col. 4, line 48). As a matter of black-letter patent law, "[w]here a specification does not require a limitation, that limitation should not be read from the specification into the claims." Specialty Composites v. Cabot Corp., 845 F.2d 981, 987 (Fed Cir. 1988) (emphasis in original); see also, E.I. DuPont de Nemours & Co. v. Phillips Petroleum Co., 849 F.2d 1430, 1433 (Fed. Cir. 1988) (improper to read limitation from specification into claim); Loctite Corp. v. Ultraseal, Ltd., 781 F.2d 861, 867 (Fed. Cir. 1985). The broad claims of the Hellman-Merkle do not require the key pair to be generated using the knapsack problem, but rather, cover any implementation of the system where "the secret key is directly related to and computationally infeasable to generate from the public key" (Omura Decl. Exh. B at Col. 19, lines 5-8, 42-44, Col. 19, line 67-Col. 20, lines 2, 27-29).

Second, Schlafly's charge that Hellman-Merkle is "inoperative" because knapsacks are insecure is meaningless under the patent law. To the extent that Schlafly is claiming that the patent is invalid for failure to meet the enablement requirement of 35 U.S.C. § 112, then the charge must fail even if one assumes, as Schlafly does, that all knapsacks have been proven to be insecure. Schlafly does not allege that knapsacks were insecure in 1977, when the application was filed. Compliance with the enablement requirement

of the patent statute is measured at the time the application is made. In re Glass, 492 F.2d 1228, 1232 (C.C.P.A. 1974). Advances in art made after the filing date cannot render the disclosure non-enabling. If the enablement requirement is met when the application is filed, "then the fact of that enablement was established for all time and a later change in the state of the art cannot change it." In re Hogan, 559 F.2d 595, 604 (C.C.P.A. 1977); see also United States Steel Corp. v. Phillips Petroleum Co., 865 F.2d 1247, 1251-52 (Fed. Cir. 1989).[11]

Finally, to the extent that Schlafly is asserting that the patent violates the utility requirement of 35 U.S.C. § 101, his argument also fails as a matter of law. A patented device does not need to accomplish all of the objectives stated in the specification in order to meet the requirements of § 101. Stiftung v. Renishaw PLC, 945 F.2d 1173, 1180 (Fed. Cir. 1991). In order to meet his burden on a non-utility defense, Schlafly would have to "prov[e] total incapacity by clear and convincing evidence." Moleculon Research Corp. v. CBS, Inc., 793 F.2d 1261, 1269 (Fed. Cir. 1986) (rejecting charge that patent claims were invalid because claims "would not work"). In this case, Schlafly has not provided any admissible evidence, much less evidence of "total incapacity." Even Schlafly's allegations about the inoperability of the knapsack

---

[11] This rule is specifically intended to preserve the right to obtain broad claims for pioneering inventions. "As pioneers . . . they would deserve broad claims to the broad concept. . . . If later states of the art could be employed as a basis for rejection under 35 U.S.C. 112, the opportunity for obtaining a basic patent upon early disclosure of pioneer inventions would be abolished." In re Hogan, 559 F.2d at 606.

implementation do not suggest that the broad claims of Hellman-Merkle do not work.

CONCLUSION

Schlafly has not presented any admissible evidence—much less clear and convincing evidence—that the Hellman-Merkle and Diffie-Hellman patents are invalid for any of the reasons asserted. Indeed, the facts and the law associated with these claims establish that CKC is entitled to judgment on these claims as a matter of law.

Dated: November 15, 1995

MICHAEL M. CARLSON
BRYAN J. WILSON
JANA G. GOLD
Morrison & Foerster

By: _____
Jana G. Gold
Attorneys for
Intervenor/Defendant
CARO-KANN CORPORATION

PROOF OF PERSONAL SERVICE
(FRCivP 5(b))

I am employed with the law firm of Morrison & Foerster, whose address is 755 Page Mill Road, Palo Alto, California 94304; I am not a party to the within cause; I am over the age of eighteen years and I am readily familiar with Morrison & Foerster's practice for the collection and processing of documents for hand delivery and know that in the ordinary course of Morrison & Foerster's business practice the document(s) described below will be taken from Morrison & Foerster's mailroom and hand delivered to the document's addressee (or left with an employee or person in charge of the addressee's office) on the same date that it is placed at Morrison & Foerster's mailroom.

I further declare that on the date hereof I served a copy of:

CKC'S OPPOSITION TO SCHLAFLY'S MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

CKC'S OBJECTIONS TO EVIDENCE SUBMITTED BY SCHLAFLY IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

DECLARATION OF JANA G. GOLD IN OPPOSITION TO SCHLAFLY'S MOTION AND IN SUPPORT OF CKC'S CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENT

DECLARATION OF DR. JIMMY OMURA IN OPPOSITION TO SCHLAFLY'S MOTION AND IN SUPPORT OF CKC'S CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

[PROPOSED] ORDER RE SCHLAFLY MOTION FOR SUMMARY JUDGMENT AND CKC CROSS-MOTION FOR SUMMARY JDUGMENT ON THE VALIDITY OF THE STANFORD PATENTS

on the following by placing a true copy thereof enclosed in a sealed envelope addressed as follows for collection and delivery at the mailroom of Morrison & Foerster, 755 Page Mill Road, Palo Alto, California 94304, in accordance with Morrison & Foerster's ordinary business practices:

James R. Busselle, Esq.
Thomas E. Moore III, Esq.
Tomlinson, Zisko, Morosoli & Maser
200 Page Mill Road
Palo Alto, CA 94306

Thomas R. Hogan, Esq.
Law Offices of Thomas R. Hogan
60 South Market Street, Suite 1125
San Jose, CA 95113-2332

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed at Palo Alto, California, on November 15, 1995.

Frances Macias Sagapolu
(typed)

(signature)

pa-16083

PROOF OF SERVICE BY OVERNIGHT DELIVERY
(CCP 1013(c), 2015.5)

I declare that I am employed with the law firm of Morrison & Foerster, whose address is 755 Page Mill Road, Palo Alto, California 94304; I am not a party to the within cause; I am over the age of eighteen years and I am readily familiar with Morrison & Foerster's practice for collection and processing of correspondence for overnight delivery and know that in the ordinary course of Morrison & Foerster's business practice the document described below will be deposited in a box or other facility regularly maintained by **U.S. Express Mail** or delivered to an authorized courier or driver authorized by **U.S. Express Mail** to receive documents on the same date that it is placed at Morrison & Foerster for collection.

I further declare that on the date hereof I served a copy of:

CKC'S OPPOSITION TO SCHLAFLY'S MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

CKC'S OBJECTIONS TO EVIDENCE SUBMITTED BY SCHLAFLY IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

DECLARATION OF JANA G. GOLD IN OPPOSITION TO SCHLAFLY'S MOTION AND IN SUPPORT OF CKC'S CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENT

DECLARATION OF DR. JIMMY OMURA IN OPPOSITION TO SCHLAFLY'S MOTION AND IN SUPPORT OF CKC'S CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

[PROPOSED] ORDER RE SCHLAFLY MOTION FOR SUMMARY JUDGMENT AND CKC CROSS-MOTION FOR SUMMARY JUDGMENT ON THE VALIDITY OF THE STANFORD PATENTS

on the following by placing a true copy thereof enclosed in a sealed envelope with delivery fees provided for, addressed as follows for collection by **U.S. Express Mail** at Morrison & Foerster, 755 Page Mill Road, Palo Alto, California 94304, in accordance with Morrison & Foerster's ordinary business practices:

Mr. Roger Schlafly
P.O. Box 1680
Soquel, California 95073

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed at Palo Alto, California, on November 15, 1995.

Frances Macias Sagapolu
(typed)

(signature)

pa-16085